AO 106 (Rev. 04/10) Application for a Search Warrant AUTHORIZED AND APPROVED/DATE: CB 5/15/25

amg 5/15/25

UNITED STATES DISTRICT COURT

for the

Western District of Oklahoma

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A Samsung Cellular Telephone in a Black Rubber Case (Target Telephone 1)

Case No. M-25-318-AMG

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Western District of Oklahoma, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841	Possession with Intent to Distribute Marijuana
21 U.S.C. § 846	Conspiracy to Distribute and Possess with Intent to Distribute Marijuana

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Stuart Talbot, FBI Task Force Officer
Printed name and title

Sworn to before me and signed in my presence.

Date: 5/15/25

Judge's signature

City and state: Oklahoma City, Oklahoma

Amanda Maxfield Green, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR WARRANTS TO SEARCH AND SEIZE ELECTRONIC DEVICES

I, Stuart Talbot, being duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for search warrants authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. Your affiant joined the Caddo Parish Sheriff's Office (CPSO) as a Deputy Sheriff on August 11, 1993. Your affiant is an "investigative or law enforcement officer" of the United States as defined in Title 18, Section 2510(7) of the United States Code. Your affiant is an officer of the United States having been deputized by the Federal Bureau of Investigation (FBI) and empowered to conduct investigations and to make arrests for offenses enumerated in Title 18, Section 2516, of the United States Code. In 2006, your affiant was assigned to the FBI New Orleans Field Office, Shreveport Resident Agency. Your affiant is a member of the FBI's Northwest Louisiana Violent Crimes Task Force (Task Force). As a Deputy Sheriff, your affiant has worked in Corrections, Patrol, and Investigations and is currently in Narcotics. Your affiant has participated in investigations of narcotics violations and violent felony crimes. Your affiant has conducted investigations utilizing complex investigative techniques and the utilization of analytical methods during

homicide, aggravated assault, aggravated battery, fraud, narcotic and theft investigations.

3. While attending the Bellevue Regional Training Academy in 1993, your affiant received training in criminal law, criminal procedure, search and seizure, narcotics investigations, firearms and use of force as well as other disciplines in law enforcement. In the course of his career, your affiant has received training in numerous areas, including but not limited to, narcotics trafficking, criminal organizations, and money laundering. At CPSO and the FBI, your affiant has participated in investigations that involved undercover officers, confidential sources, cooperating witnesses, physical surveillance, PEN registers, trap and trace devices, toll analyses, CCTV surveillance, consensual recordings and monitoring, drug evidence purchases, service of search warrants, service of arrest warrants, subject interviews, and wiretaps.

4. Your affiant investigated criminal organizations operating within the United States relating to violations of both Title 18 and Title 21 of the United States Code. Your affiant has worked with confidential sources and cooperating witnesses whose information has resulted in the arrest and conviction of individuals based on federal crimes.

5. Your affiant is currently assigned to the Task Force that includes federal, state and local officers investigating illegal gang activity, crimes of violence and drug trafficking organizations in Northwest Louisiana.

6. The statements contained in this affidavit are based on my personal knowledge, as well as information I have received from other law enforcement personnel and other persons with knowledge of the relevant facts. I have not set forth all facts learned during the course of this investigation, but only those facts necessary to establish probable cause for the issuance of the requested search warrants.

IDENTIFICATION OF DEVICES TO BE EXAMINED

7. The property to be searched include the following devices more particularly described in Attachment A:

a. A Samsung cellular telephone, in a black rubber case ("**TARGET TELEPHONE 1**");

b. A grey Motorola Moto G 5G-2024 cellular telephone ("**TARGET TELEPHONE 2**"); and

c. A light green iPhone cellular telephone ("**TARGET TELEPHONE 3**")

8. The warrants would also permit law enforcement to obtain from **Adham DEEB**, the individual from whom **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET TELEPHONE 3** were seized, the display of his biometric characteristic (i.e., fingerprint, thumbprint, and/or facial characteristics) to unlock **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET TELEPHONE 3**.

9. **TARGET TELEPHONE 1, TARGET TELEPHONE 2,** and **TARGET TELEPHONE 3** are in the custody of the FBI and are presently located in the Western District of Oklahoma.

10. As will be explained more below, there is probable cause to believe that violations of Title 21, United States Code, Sections 841 and 846 have been committed. Additionally, there is probable cause to believe that evidence of those violations, as more particularly described in Attachment B, will be found on **TARGET TELEPHONE 1, TARGET TELEPHONE 2,** and **TARGET TELEPHONE 3.**

PROBABLE CAUSE

INVESTIGATIVE AND PROCEDURAL BACKGROUND

11. In November of 2018, the FBI's Northwest Louisiana Violent Crimes Task Force began investigating Step or Die (SOD), a local violent gang in Shreveport, Louisiana, for illegal drug trafficking and other violent crimes. Through the investigation, agents determined that Hikmat Deeb ("H. Deeb") and Brieon O'Neal were marijuana sources of supply to SOD.

12. FBI then began investigating H. Deeb and O'Neal for illegal drug trafficking. The investigation included, but was not limited to, court-ordered Title III wiretaps on two cellular telephone numbers utilized by H. Deeb.

13. The investigation confirmed that H. Deeb was obtaining large quantities of marijuana from sources of supply in Oklahoma (and previously,

California) and having the drugs transported to the Western District of Louisiana and elsewhere for further distribution.

14. The investigation implicated numerous co-conspirators. Rshad Deeb and **Adham DEEB, a.k.a. "Polo"** (hereinafter **A. DEEB**) are two of H. Deeb's brothers. Both were identified as obtaining, distributing, and facilitating the distribution of marijuana to H. Deeb and others.

15. On September 6, 2023, **A. DEEB** was charged by indictment in the Western District of Louisiana with Conspiracy to Distribute and Possess with Intent to Distribute 100 Kilograms of Marijuana. An arrest warrant was issued that same day.

16. On October 17, 2023, your affiant attempted to execute the warrant. Your affiant went to **A. DEEB's** residence located at 1111 Lincoln Green, Norman, Oklahoma and advised his mother, Amal Rashed, of the arrest warrant. Your affiant then spoke to **A. DEEB** by phone[1] and similarly advised him of the warrant. **A. DEEB** did not, however, surrender to authorities.[2]

---

[1] Your affiant contacted **A. DEEB** on cellular telephone number (929) 308-1325. Your affiant identified this number as being utilized by **A. DEEB** through the Title III interceptions.

[2] It is also noted that, on October 25, 2023, the United States Attorney's Office for the Western District of Louisiana was contacted by an attorney on behalf of **A. DEEB**. The attorney advised he was in the process of being retained by **A. DEEB** and, upon doing so, would coordinate **A. DEEB's** surrender to the United States Marshal's Service (USMS). The attorney was never retained by **A. DEEB**, however, and **A. DEEB** still did not surrender to authorities. On November 1, 2023, the United States Attorney's Office was contacted by a second attorney who similarly advised he would be enrolling in the criminal case on behalf of **A. DEEB**. The attorney was never retained by **A. DEEB**, however, and **A. DEEB** still did not surrender to authorities. Your affiant provides this information to demonstrate that **A. DEEB** knew of the federal arrest warrant.

17. **A. DEEB** remained a fugitive until April 1, 2025, at which time USMS deputies located and arrested him at a gas station in Edmond, Oklahoma. **A. DEEB** was driving a vehicle registered to Jaqueline Ornelas.[3] United States Marshal's deputies seized **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET TELEPHONE 3** from **A. DEEB**. According to the Deputy Marshal who made the arrest, all phones were in the vehicle. **A. DEEB** identified all phones as belonging to him.

EVIDENCE OF A. DEEB'S CONTINUED ILLEGAL ACTIVITIES

18. Your affiant has become aware that, during his abscondence, **A. DEEB** continued to engage in illegal drug trafficking and used multiple cellular telephones to do so.

19. On or about January 24, 2025, an individual named Lamarquez Harris, a.k.a. "Quez" was arrested for possession of a firearm by a convicted felon and possession with the intent to distribute marijuana. In addition to marijuana and a firearm, arresting officers seized two cell phones.

20. At the time of his arrest, Harris was on supervised release in the Western District of Louisiana for Possession of a Firearm by a Convicted Felon. *United States v. Lamarquez Harris*, 5:20-cr-00073. And so, on February 18, 2025, agents obtained federal search warrants for Harris' cell phones. Agents located numerous messages between Harris and Jerusalia

[3] Ornelas is the wife of Rshad Deeb.

Bell.[4] The messages occurred over Signal, end-to-end encrypted application, and suggested Bell was supplying Harris with marijuana. For example, in a series of messages on October 31, 2024, Bell sent 12 videos/images of marijuana to Harris. Harris asked, "what these going for and where they at". Bell responded, "975 and up and in Longview 45 minutes from you".

21. Based upon the messages located on Harris' phone, on February 25, 2025, agents obtained a search warrant for Bell's iCloud account. Through a review of messages located on the account, agents identified at least three telephone numbers being utilized by **A. DEEB**: (213) 255-8808[5], (214) 223-3134[6], and (929) 308-1325[7]. Messages between Bell and **A. DEEB** were indicative of drug trafficking.

22. For example, on October 28, 2024, Bell sent a message to **A. DEEB** on telephone number (213) 255-8808 stating "I got someone trying to

---

[4] Bell is the wife of H. Deeb and a co-defendant. She was allowed to remain on an unsecured bond for the pendency of the criminal case.

[5] Agents identified this telephone number as being utilized by **A. DEEB** through a WhatsApp message sent on September 26, 2024. Specifically, the individual utilizing this number identified himself as "**Polo**". Agents also identified this telephone number as being associated with **A. DEEB** through a string of text messages between Bell and Harris. Specifically, on November 6, 2024, Harris complained to Bell that "**Polo** did some fuck shit sis because I sent him some money to end me some shit cuz..." The next day, on November 7, 2024, Bell asked Harris "How much did you send him"? Harris replied, "I sent him 300 for my shipping." That same day, Bell sent a message via Whats App to this telephone number stating, "Quez said you got him for $300".

[6] Agents identified this telephone number as being utilized by **A. DEEB** through a text message on January 22, 2025. Like the WhatsApp message referenced in Footnote 4, the individual utilizing this number identified himself as "**Polo**".

[7] Agents identified this telephone number as being utilized by **A. DEEB** because Bell saved the contact for this telephone number as "**Adham Deeb**."

get 50 pairs". Your affiant knows from training and experience that "pairs" is a street term for "pounds."

23. The next day, on October 29, 2024, **A. DEEB** and Bell exchanged the following text messages:

Bell:	Don't forget to send me that menu. He trying to go today.
A. DEEB:	Good morning. Sorry. It was 4 AM. And pretty much same shit. Runtz and that good stuff. Just let me know when he wants to go I got it set up.
Bell:	Yeah. He wants a menu with prices so he knows how much he needs to bring and he wants to go today.
A. DEEB:	Ok. I'm done from the gym in one hour then gonna call you. *It's in my other phone.* [Emphasis added].
Bell:	Ok.

Your affiant knows from underlying investigation that "Runtz" is a strain of marijuana. Your affiant therefore believes Bell had a customer wanting to obtain 50 pounds marijuana from **A. DEEB** and/or a source of supply connected to him. **A. DEEB** replied there were "Runtz" and other strains of marijuana available for purchase, and that the list of other strains as well as their prices were contained on his other telephone.

PROCEDURES FOR ELECTRONICALLY STORED INFORMATION

24. It is not possible to determine, merely by knowing the cellular telephone's make, model and serial number, the nature and types of services to which the device is subscribed and the nature of the data stored on the device. Cellular devices today may have a broad range of functionality, for

example the devices may (1) be simple cellular telephones and text message devices, (2) include cameras, (3) serve as personal digital assistants, (4) have functions such as calendars and full address books, and (5) be mini computers allowing for electronic mail services, web services, and rudimentary word processing. An increasing number of cellular service providers now allow for their subscribers to access their device over the internet and remotely destroy all the data contained on the device. For that reason, the device may only be powered in a secure environment or, if possible, started in "flight mode" which disables access to the network. Unlike typical computers, many cellular telephones do not have hard drives or hard drive equivalents and store information in volatile memory within the device or in memory cards inserted into the device. Current technology provides some solutions for acquiring some of the data stored in some cellular telephone models using forensic hardware and software. Even if some of the stored information on the device may be acquired forensically, not all the data subject to seizure may be so acquired. For devices that are not subject to forensic data acquisition or that have potentially relevant data stored that is not subject to such acquisition, the examiner must inspect the device manually and record the process and the results using digital photography. This process is time and labor intensive and may take weeks or longer.

25. Following the issuance of these warrants, I will have **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET**

TELEPHONE 3 forensically analyzed. All forensic analysis of the data contained within the telephones and the memory cards will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant.

26. Identifying and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including manual review, and, consequently, may take weeks or months. The personnel conducting the identification and extraction of data will complete the analysis within 90 days, absent further application to this court.

BIOMETRIC UNLOCK REQUEST

27. As state above, the warrants I am applying for would permit law enforcement to obtain from **Adham DEEB, a.k.a. "Polo"** the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET TELEPHONE 3** subject to search and seizure pursuant to these warrants. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password.

These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, there is probable cause to believe that **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET TELEPHONE 3** were being utilized by **A. DEEB** at the time of his arrest. The passcodes or passwords that would unlock the devices subject to search under these warrants are not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by these warrants.

f. Due to the foregoing, the warrants I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of **A. DEEB** to the fingerprint scanner of the device; and/or (2) hold the device in front of the face of **A. DEEB** and activate the facial recognition feature, for the purpose of attempting to unlock the devices in order to search their contents as authorized by these warrants.

AUTHORIZATION REQUEST

28. This investigation concerns alleged violations of 21 U.S.C. §§ 841 and 846. On the basis of the information contained in this affidavit, there is probable cause to believe that evidence of these violations will be found in **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET TELEPHONE 3**.

Task Force Officer Stuart Talbot
Federal Bureau of Investigation

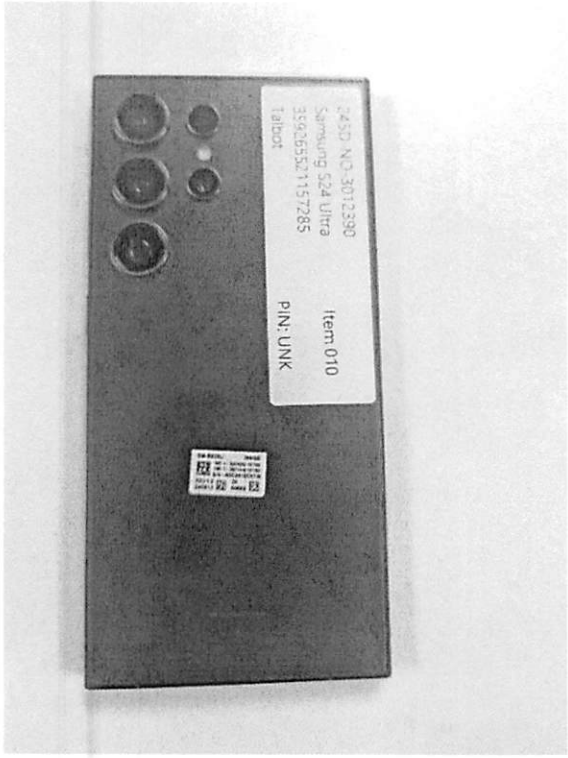
Subscribed and sworn to before me this 15th day of May 2025.

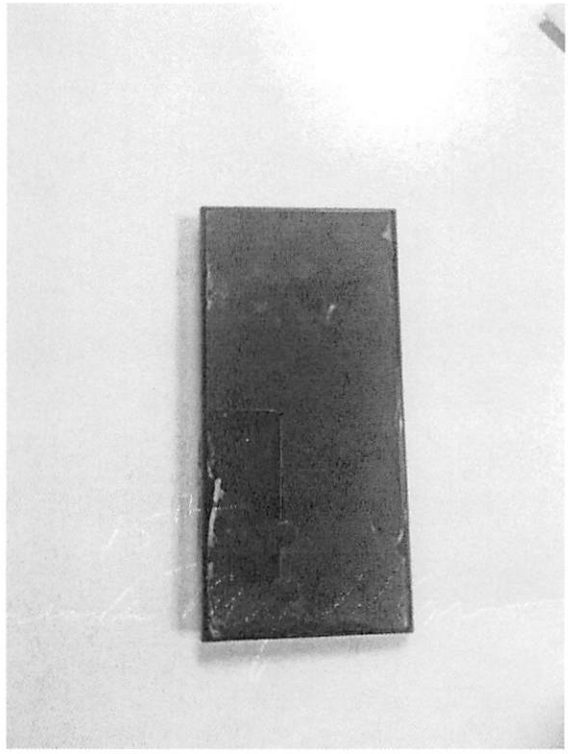
AMANDA MAXFIELD GREEN
United States Magistrate Judge

ATTACHMENT A

Property to Be Seized and Searched

TARGET TELEPHONE 1: Samsung, in black rubber case





ATTACHMENT B

Particular Things to be Seized

All records relating to violations of Title 21, United States Code, Sections 841(a)(1) and 846:

1. Records relating to communication with others as to the criminal offenses listed above; including incoming and outgoing voice messages; text messages; emails; multimedia messages; applications that serve to allow parties to communicate, including but not limited to WhatsApp, Signal, Snapchat; all call logs; secondary phone number accounts, including those derived from Skype, Line 2, Google Voice, and other applications that can assign roaming phone numbers; and other Internet-based communication media;

2. Records relating to documentation or memorialization of the criminal offenses listed above, including voice memos, photographs, videos, and other audio and video media, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos, including device information, geotagging information, and information about the creation date of the audio and video media;

3. Records relating to the planning and execution of the criminal offenses above, including Internet activity, firewall logs, caches, browser history, and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search

engine, records of user-typed web addresses, account information, settings, and saved usage information;

4. Application data relating to the criminal offenses listed above;

5. All bank records, checks, credit card bills, account information, and other financial records;

6. Evidence of user attribution showing who used or owned **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET TELEPHONE 3** at the time the described in this warrant were created, edited, or deleted, such as logs, phone books, saved usernames and passwords, documents, and browsing history;

7. All records and information related to the geolocation of **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET TELEPHONE 3** and travel in furtherance of the criminal offense listed above; and

8. All records and information related to the coordination, agreement, collaboration, and concerted effort of and with others to violate the criminal statutes listed above.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage.

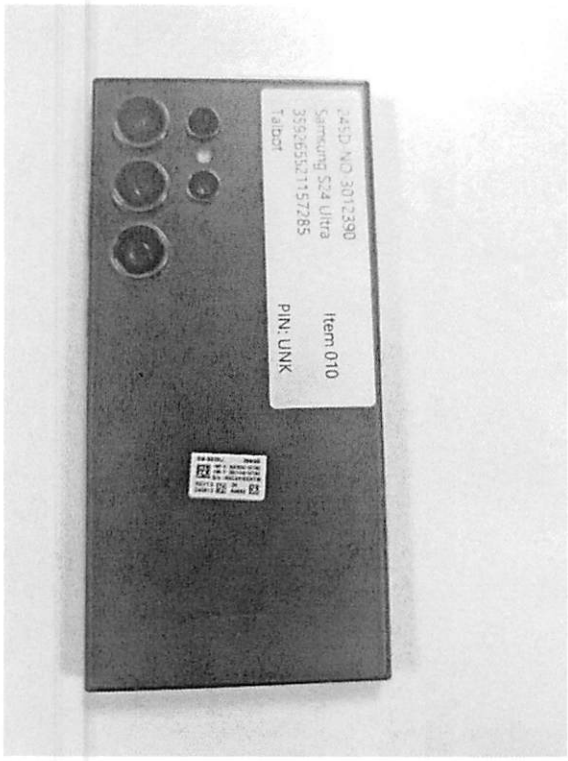
This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

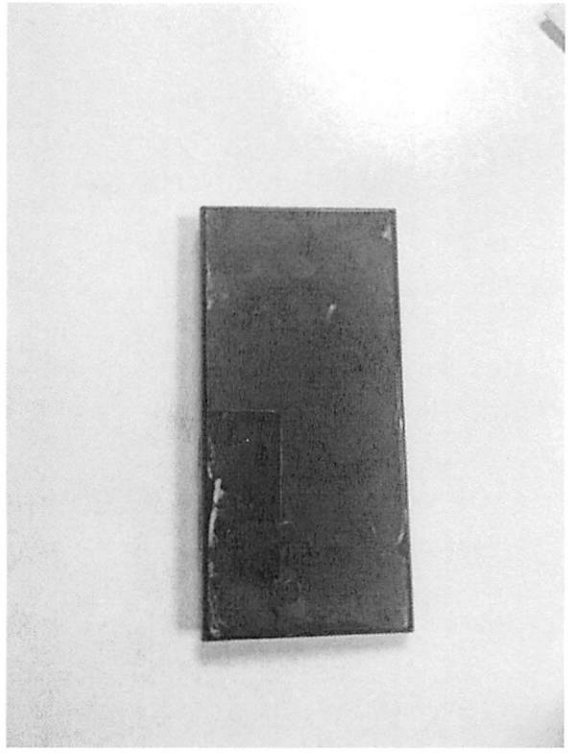
Additionally, during the execution of the search of **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET TELEPHONE 3** described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of **Adham DEEB, a.k.a. "Polo,"** who is reasonably believed by law enforcement to be a user of **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET TELEPHONE 3**, to the fingerprint scanner of the devices; (2) hold **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET TELEPHONE 3** in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

ATTACHMENT A

Property to Be Seized and Searched

TARGET TELEPHONE 1: Samsung, in black rubber case





ATTACHMENT B

Particular Things to be Seized

All records relating to violations of Title 21, United States Code, Sections 841(a)(1) and 846:

1. Records relating to communication with others as to the criminal offenses listed above; including incoming and outgoing voice messages; text messages; emails; multimedia messages; applications that serve to allow parties to communicate, including but not limited to WhatsApp, Signal, Snapchat; all call logs; secondary phone number accounts, including those derived from Skype, Line 2, Google Voice, and other applications that can assign roaming phone numbers; and other Internet-based communication media;

2. Records relating to documentation or memorialization of the criminal offenses listed above, including voice memos, photographs, videos, and other audio and video media, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos, including device information, geotagging information, and information about the creation date of the audio and video media;

3. Records relating to the planning and execution of the criminal offenses above, including Internet activity, firewall logs, caches, browser history, and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search

engine, records of user-typed web addresses, account information, settings, and saved usage information;

4. Application data relating to the criminal offenses listed above;

5. All bank records, checks, credit card bills, account information, and other financial records;

6. Evidence of user attribution showing who used or owned **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET TELEPHONE 3** at the time the described in this warrant were created, edited, or deleted, such as logs, phone books, saved usernames and passwords, documents, and browsing history;

7. All records and information related to the geolocation of **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET TELEPHONE 3** and travel in furtherance of the criminal offense listed above; and

8. All records and information related to the coordination, agreement, collaboration, and concerted effort of and with others to violate the criminal statutes listed above.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

Additionally, during the execution of the search of **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET TELEPHONE 3** described in Attachment A, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of **Adham DEEB, a.k.a. "Polo,"** who is reasonably believed by law enforcement to be a user of **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET TELEPHONE 3**, to the fingerprint scanner of the devices; (2) hold **TARGET TELEPHONE 1**, **TARGET TELEPHONE 2**, and **TARGET TELEPHONE 3** in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.